Great — let's go step by step. **Prefilter Policies** in **Cisco FMC (Firepower Management Center)** are a powerful but often misunderstood feature. They allow you to **quickly filter traffic at an early stage**, **before deep packet inspection**, saving processing resources on the firewall.

What is a Prefilter Policy?

Prefilter Policy is the **first line of filtering** on a Firepower Threat Defense (FTD) device. It is processed **before**:

- Access Control Policy
- Intrusion policies (IPS)
- Application inspection
- URL filtering
- File/malware inspection

Goal: Quickly decide whether to **allow**, **block**, or **fastpath (bypass inspection)** for certain types of traffic.

Why Use Prefilter Policies?

- Improve **performance** by filtering obvious traffic early.
- Avoid unnecessary **deep inspection** for trusted or unimportant traffic.
- Block **unwanted traffic** like VPNs, P2P, or IPs from specific countries quickly.
- Create **VPN tunnels** or **tunnel zones** using **Security Intelligence** or **tunnel rules**.

Prefilter Policy Architecture

A **Prefilter Policy** contains two major types of rules:

Rule Type	Purpose
Tunnel Rules	For VPN tunnel traffic, GRE, IPSec, etc.
Prefilter Rules	General early filtering based on IP, port, VLAN, etc.

✅ Step-by-Step Guide: Create and Apply Prefilter Policy

🔹 Step 1: Create Network/Port Objects (Reusable)

🌐 Network Object

1. Go to **Objects > Object Management > Network**.
2. Click **Add Network**.
3. Set:
    - Name: `Blocked_IP_Range`
    - Type: `Network`
    - Value: `192.168.50.0/24`
    - Save.

🔌 Port Object

1. Go to **Objects > Object Management > Ports**
2. Add: `TCP`, `UDP`, or custom ports like `TCP/445` or `UDP/53`.

🔹 Step 2: Create Prefilter Policy

1. Navigate to:
   Policies > Prefilter
   Click **New Policy** or edit existing one.
2. Name it: `Prefilter_Block_Untrusted`.
3. Set default action:
    - **Analyze** (send unmatched traffic to ACP)
    - **Block** (drop all unmatched traffic — very strict)
4. Save the policy.

🔹 Step 3: Add a Prefilter Rule

1. Inside the prefilter policy, click **Add Rule**.
2. **Rule Types**:
    - Choose **Prefilter Rule** (unless filtering tunnels).
3. Fill in:
    - **Name**: `Block Untrusted Network`
    - **Source Networks**: Select `Blocked_IP_Range` (created earlier).
    - **Destination**: `Any`
    - **VLAN Tags / Interfaces**: Optional
    - **Ports / Protocols**: Optional

    - **Action**: Choose:
        - **Block** – Drops traffic immediately
        - **Fastpath** – Allows traffic without inspection
        - **Analyze** – Send to Access Control Policy (normal path)
    - **Logging**: Enable logging at **beginning** for visibility.
4. Save the rule.

✅ Step 4: Apply Prefilter to Access Control Policy

1. Go to:
   Policies > Access Control > Open your ACP.
2. Under **Policy Information**, set:
    - **Prefilter Policy**: Choose `Prefilter_Block_Untrusted`.
3. Click **Save**.

✅ Step 5: Deploy to FTD Devices

1. Click **Deploy** (top right).
2. Choose the relevant FTDs and deploy.

🔍 Rule Actions Explained

Action	Description
Block	Immediately drops packets matching rule (no further inspection).
Fastpath	Allows traffic to bypass deep inspection — good for trusted/internal traffic.
Analyze	Sends traffic to ACP for full inspection.
Monitor Only	Logs traffic but does not affect flow. Used for visibility/testing.

🧪 Example Use Cases

🚫 Block a Suspicious IP Range

- Rule: Source = `203.0.113.0/24`, Action = **Block**

🚀 Fastpath for Internal Backup Server

- Rule: Source = `10.0.1.10`, Destination = `10.0.2.10`, Port = `TCP/445`, Action = **Fastpath**

Inspect All VPN Tunnel Traffic

- Tunnel Rule: GRE or IPSec, Action = **Analyze**

Tips and Best Practices

- Use **Fastpath** for trusted internal services to save CPU.
- Place **Block rules** at the top.
- Keep **rules specific** — don't use large "any-any" blocks unless absolutely needed.
- Monitor rule hits under **Analysis > Connections > Prefilter Events**.

Would you like a **visual diagram**, **exportable example config**, or help with **VPN tunnel filtering rules** next?

Slide 1: Title Slide

Title: Prefiltering and Prefilter Policies

Subtitle: Enhancing Network Performance and Security

Image: Network security or firewall icon

Slide 2: Chapter Contents

- About Prefiltering
- Best Practices for Prefiltering
- Encapsulated Traffic Handling
- Requirements for Prefilter Policies

- Configuring Prefiltering
- Tunnel Zones and Prefiltering
- Prefilter Policy Hit Counts
- Large Flow Offloads

Slide 3: About Prefiltering

Definition:

- First phase of access control, fast and simple.
- Uses **outer-header criteria** for quick traffic handling.

Benefits:

- **Improves performance** by excluding non-inspected traffic early.
- **Tailors deep inspection** for encapsulated traffic (e.g., tunnels).

Key Difference:

- Prefiltering: Fast, outer-header checks.
- Access Control: Deep, inner-header inspection.

Slide 4: Prefiltering vs. Access Control

Feature	Prefiltering	Access Control
Function	Fastpath/Block early	Full inspection & control
Actions	Fastpath, Block, Analyze	Trust, Block, Monitor, etc.
Rule Criteria	IP, VLAN, Port, Protocol	User, App, URL, deep inspection

Feature	Prefiltering	Access Control
Logging	Fastpath/Block only	All connections

Slide 5: Best Practices for Prefiltering

Ideal for Fastpathing:

- Site-to-site VPN passthrough traffic
- Scanner traffic (reduces false positives)
- Voice/Video/Backup traffic

Model Support:

- **Only for Firepower Threat Defense (FTD)**.
- For non-FTD devices, use early **Trust/Block rules** in access control.

Slide 6: Encapsulated Traffic Handling

Supported Protocols:

- GRE, PPTP, IPinIP, IPv6inIP, Teredo

Limitations:

- GRE v1/PPTP bypass outer flow processing.
- No HA/clustering replication for passenger flows.
- GRE v0 must have optional sequence numbers.

References:

- RFCs 1701, 2784 (GRE)
- RFC 2637 (PPTP)

Slide 7: Configuring Prefiltering

Steps:

1. **Create Policy**: `Policies > Access Control > Prefilter` → New Policy.
2. **Set Default Action**: Block or Analyze tunnels.
3. **Add Rules**:
   - Tunnel rules (rezoning).
   - Prefilter rules (fastpath/block).
4. **Associate with Access Control Policy**.
5. **Deploy Changes**.

Note:

- Existing sessions ignore new prefilter rules until cleared.

Slide 8: Tunnel Zones and Prefiltering

Purpose:

- Rezone tunnels to group encapsulated connections for tailored inspection.

Example Workflow:

1. Assign tunnel zone in prefilter policy (e.g., `GRE_tunnel`).
2. Use zone as **source constraint** in access control rules.

Caution:

- Rezoned traffic **ignores original security zones**.

Slide 9: Prefilter Policy Hit Counts

What It Tracks:

- Number of times a rule matches traffic.

Viewing:

- Use **Policy Hit Counts** in monitoring dashboards.

Slide 10: Large Flow Offloads

Purpose:

- Hardware acceleration for high-throughput traffic (e.g., backups, HFT).

Supported Flows:

- **Static**: Fastpath rules (TCP/UDP/GRE).
- **Dynamic**: Trusted flows (e.g., SSL bypass, IAB).

Limitations:

- IPv4 only. No support for inline/IPv6/IPsec.
- Disabled if TCP state bypass is active.

Slide 11: Summary

- Prefiltering **optimizes performance** via early traffic handling.
- Tunnel zones enable **granular control** of encapsulated traffic.
- Large flow offloads boost throughput for data-intensive apps.

Next Steps:

- Configure prefilter policies for critical traffic.
- Monitor hit counts and adjust rules.

Slide 12: Q&A

Questions?
Contact: [Your Team/Email]

Design Tips:

- Use **icons** for protocols (GRE, VPN).
- Highlight **caution points** in red.
- Include a **flowchart** for prefilter workflow (optional).

Let me know if you'd like any modifications!